IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF [redacted]

Criminal No. 1:22-SW- 245

UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE

I, Laura Calvillo, a Special Agent with the Federal Bureau of Investigation (FBI), Washington Field Division, Washington, D.C., being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the FBI and have been since March of 2016. I am currently assigned to the Washington Field Office, Northern Virginia Resident Agency. Prior to joining the FBI, I was a Special Agent for the U.S. Army Criminal Investigation Division and assigned to investigate violations of federal law to include violations involving child pornography and the sexual exploitation of children. Currently, as an FBI Special Agent, I investigate federal violations concerning kidnapping, child pornography, the sexual exploitation of children, human trafficking, and related offenses. I have gained experience through training and work related to conducting these types of investigations. I am a trained and certified digital extraction technician for the FBI.

2. Moreover, I am a law enforcement officer who is engaged in enforcing criminal laws, including offenses in violation of Title 18, U.S. Code, Sections 2251(a) and

(e) (attempted production and production of child pornography), 2252(a)(1)(transportation of child pornography), 2252(a)(2), distribution and receipt of child pornography, 2252(a)(4)(B) (possession and access with intent to view child pornography), 2422(b) (enticement and attempted enticement of a minor), and 1591(a) (sex trafficking of a minor). As such, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rule of Criminal Procedure for a warrant to search the entire premises located at [redacted] (hereinafter, the "**SUBJECT PREMISES**")—which is more particularly described in Attachment A—for the things described in Attachment B.

4. I am familiar with the information contained in this affidavit based upon the investigation I have conducted, which includes conversations with other law enforcement officers and others and review of reports and database records. Because I submit this affidavit for the limited purpose of establishing that there is sufficient probable cause for the requested warrant, I have not included each and every fact known to me or the government.

5. Based on my training and experience and the facts set forth in this affidavit, I submit that there is probable cause to believe that violations of Title 18, U.S. Code, Sections 2252(a)(1) (transportation of child pornography), 2252(a)(2) (receipt and distribution of child pornography), and 2252(a)(4)(B) (possession of child pornography) (collectively, the "Target Offenses") have been committed by James Meek. There also is probable cause to search the

SUBJECT PREMISES described in Attachment A for evidence, instrumentalities, contraband, and fruits of the Target Offenses as further described in Attachment B.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as used in this affidavit, is any visual depiction of sexually explicit conduct where the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct.

c. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, flash drives or thumb drives, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices,

mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. A "wireless telephone," or mobile or cellular telephone, is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

f. A "tablet" is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "Wi-Fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. A "storage medium" is any physical object upon which computer data can be recorded. Examples include thumb drives, external hard drives, RAM, floppy disks, flash memory, CD-ROMs, DVDs, and other magnetic or optical media.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Wireless routers" create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

j. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the internet service provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if

an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

k. ISPs, as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

l. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

m. "Records," "documents," and "materials," as used herein, include all information recorded in any form and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

n. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

o. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

SUMMARY OF PROBABLE CAUSE

7. This Application for a search warrant stems from an investigative lead sent to the Washington Field Office's Child Exploitation and Human Trafficking Task Force. The lead

stated that on March 11, 2021, Dropbox filed a CyberTip with the National Center for Missing and Exploited Children (NCMEC) regarding child pornography found in a Dropbox account on March 10, 2021. The username associated with the account was "James Meek," User ID [redacted] and the email address associated with the account was [redacted] The tip also provided two IP addresses: [redacted] (which Dropbox's tip indicated had been used on 11 occasions between August 4, 2020 and February 16, 2021) and [redacted] (which Dropbox's tip indicated had been used once, on June 16, 2020). At the time, the ISP associated with these two IP addresses was Verizon. Dropbox viewed the images of child pornography before submitting them to NCMEC.

A. Records Obtained by Virginia State Police and the FBI Based on the CyberTip

8. On June 23, 2021, a law enforcement officer with the Virginia State Police served an administrative subpoena on Verizon for information associated with IP address [redacted] on June 16, 2020 (at 0436 hours UTC), and IP address [redacted] between August 4, 2020 (at 1840 hours UTC) and February 16, 2021 (at 2032 hours UTC).

9. On July 7, 2021, Verizon responded with information that from June 5, 2020 (at 1827 UTC) to July 22, 2020 (at 2217 UTC), IP address [redacted] was assigned to James Meek, at the **SUBJECT PREMISES**, with email address [redacted] and telephone number [redacted] Verizon also responded that from July 22, 2020 (at 2234 UTC) to July 7, 2021, IP address [redacted] was also assigned to James Meek, at the **SUBJECT PREMISES** with the same email address and telephone number.

10. On June 23, 2021, a law enforcement officer with the Virginia State Police served an administrative subpoena to Google for information associated with the email account [redacted]

11. On June 25, 2021, Google responded that the subscriber name associated with that gmail account is [redacted]" the recovery email address was [redacted] and the recovery text number was [redacted] Google also provided the following billing information for the subscriber: James G Meek, the **SUBJECT PREMISES**, and the telephone number [redacted] The most recent credit card on file was a Mastercard [redacted], expiration date [redacted] with the same billing name and address.

12. On June 23, 2021, at 21:06:23 UTC, the Google account [redacted]com used IP address [redacted] to log in to the Google account.

13. On or about November 16, 2021, Verizon provided the FBI with records for the telephone number [redacted] A review of those records revealed that the subscriber for the account associated with that telephone number was James Meek, whose billing address was the **SUBJECT PREMISES** and email address was [redacted] The service for that telephone number started on or about February 11, 2011. The cellular telephone connected to this account was an iPhone 11 with IMEI [redacted] and that device had been associated with the account since August 4, 2020.

14. On or about November 18, 2021, Google provided records in response to a court order that the Honorable John F. Anderson of the U.S. District Court of the Eastern District of Virginia had issued pursuant to 18 U.S.C. § 2703(d). A review of those records revealed that the subscriber for [redacted] s [redacted]" the recovery email address was [redacted] and the recovery text number was the telephone number [redacted] In addition, the subscriber's birthday matched Meek's date of birth as listed in Virginia Department of Motor Vehicle records. This account was accessed numerous times between

February 6, 2021, and November 8, 2021, by IP address [redacted] *i.e.*, the IP address that, according to Verizon's records, had been assigned to Meek's apartment for the period in question. Additionally, IP address records reveal that the IP address assigned to Meek's cellular telephone was used to access the Google account on November 7, 2021.

15. Virginia Department of Motor Vehicles records confirmed that Meek's home address is listed as the **SUBJECT PREMISES.**

16. The investigation has revealed that Meek is a reporter for ABC News and that he reports on national security matters.

B. The Images Reported and Viewed by Dropbox

17. Your affiant has viewed the 5 videos of child pornography that were reported and viewed by Dropbox in March 2021, and the videos all appear to depict minors engaged in sexually explicit conduct. The videos are described as follows:

a. ***Video Titled "072omstjb_4"***: This video depicts what appears to be either a prepubescent or early teenage female in a black, long-sleeve shirt and multicolored pants sitting on a floor. Based on the lack of hair on the female's genitals and the size of the individual, it appears that the female is prepubescent or in her early teenage years. The focus of the video is on her bare vagina and anus. The pubescent female digitally masturbates her vagina and anus. The video is approximately 2 minutes and 55 seconds long.

b. ***Video Titled "sex kids-07"***: This video depicts what appears to be a naked prepubescent female lying on her back. The focus of the video is a close-up of her bare vagina and pubic area. The video is approximately 47 seconds long.

c. ***Video Titled "Video 22-09-2018, 12 10 47 PM"***: This video depicts what appears to be a prepubescent female. A pair of yellow underwear with purple bows consistent

with the type of underwear worn by a child is around her thighs, exposing her buttocks. What appears to be an adult male rubs his erect penis against her buttocks. The video is approximately 7 seconds long.

d. ***Video Titled "Video 27-05-2018, 8 41 20 PM"***: This video depicts what appears to be a prepubescent female. An erect penis that appears to belong to an adult rubs on her vagina and appears to penetrate her vagina. The video is approximately 24 seconds long.

e. ***Video Titled "Video Feb 18, 4 32 16 AM"***: This video depicts what appears to be a prepubescent female wearing a yellow Minnie Mouse shirt and being orally penetrated by an erect penis. The video also shows a close-up of what appears to be a prepubescent female's bare spread vagina, which is subsequently penetrated by an erect penis which appears to be prepubescent as well. The video appears to have been edited at points due to cuts in the frames, but the prepubescent female and erect penis appear to be the same people throughout the video. The video is approximately 2 minutes and 29 seconds long.

18. The Dropbox CyberTip also provided a spreadsheet with the file path for how the videos were stored on Dropbox. One of the videos was in a folder named "trade" and another was in a folder named "Sex kids (1)". Based on my training and experience with similar investigations, it is common for possessors and traders of child pornography to organize and label their collections. The term "trade" is indicative of that person having traded the image or video with another who collects child pornography in exchange for child pornography.

19. The information from the March 2021 Dropbox CyberTip also revealed that the "James Meek" Dropbox account user added the child pornography to Dropbox or moved the child pornography between different folders within Dropbox, further suggesting

that he used Dropbox to store child pornography.

20. Based on my training and experience, it is likely that Meek uploaded the child pornography from a device connected to Dropbox in the subject's possession for ease and security of storage, and so that he could then download the child pornography from Dropbox onto other devices possessed by the subject. In light of the folder titled "trade," it is also likely that Meek uploaded the child pornography so that he could trade Dropbox links with other traders of child pornography. While the content stored in Dropbox was deleted by Dropbox, it is likely still maintained on any device used by the subject. In addition, even if the videos themselves are not still saved on one of Meek's personal device, a forensic examination of those devices could yield evidence that the of the subject having previously downloaded, accessed, or viewed these images on those devices.

C. FBI's Attempt to Obtain Records from Dropbox

21. Dropbox is a service that allows its users to store files on Dropbox's servers. These files can then be sent and/or shared with others and can be synchronized across multiple devices, including computers, phones, and tablets. Subscribers are able to access a file they have stored in Dropbox on any of their devices, as well as download, email, or share it with others.

22. On or about November 10, 2021, the Honorable John F. Anderson of the U.S. District Court for the Eastern District of Virginia issued a search warrant for Dropbox for the account associated with user name James Meek, user [redacted] and email [redacted]

23. On or about November 23, 2021, Dropbox responded it had no records to provide. Dropbox had closed the account following the discovery of child pornography, had only

preserved the contents of the account for 90 days from the date of the CyberTip, and had already deleted the account by the time the FBI submitted a preservation request on or about September 9, 2021.

D. Other CyberTips Regarding Meek

24. Meek also has been implicated in other CyberTips, which indicates ongoing involvement with child pornography. Specifically, in or around July 2016, Microsoft submitted two CyberTips to NCMEC for a Skype account that uploaded and/or shared two images of child pornography approximately eight minutes apart. The Skype user name was [redacted] and the IP address used to uploaded the files was [redacted]

25. On or about August 19, 2016, in response to requests for records relating to IP address [redacted] Verizon produced records indicating that the subscriber information associated with that IP address on or about July 9, 2016, at 14:32 and 14:40 UTC was James Meek at the **SUBJECT PREMISES** with the telephone numbe[redacted]

26. According to the Skype CyberTip, Microsoft reported and viewed two images of child pornography. I reviewed the images in question, and they both appear to depict minors engaged in sexually explicit conduct. The images are described as follows:

a. ***Image Titled "tmp8EC1"***: This image depicts what appears to be a prepubescent female with her leggings and underwear pulled down around her thighs. She is sitting in what appears to be a child's stroller with her legs lifted up exposing her vagina.

b. ***Image Titled "tmpC6AF"***: This image depicts what appears to be a nude prepubescent female sitting in a bathtub with her legs spread exposing her vagina. There is a nude adult male standing in the bathtub and urinating on the child. The image has the following caption: "Who needs a shower when you have got dads hot piss, look up so you can drink some

as well".

27. Other information further supports the attribution evidence against Meek. Specifically, investigation revealed that on or about July 28, 2020, the user name [redacted] posted a tweet. This tweet was connected to Meek because the email address used to register the Twitter account was [redacted] which was the same account used as the recovery email address for the meekwire gmail account. Additionally, the account had used IP address [redacted] to register the account on June 14, 2020 at 2:40 UTC. This IP address was the same IP address in the Dropbox CyberTip, and it was assigned to Meek from on or about June 5, 2020, to July 22, 2020.

E. Characteristics of Child Pornographers

28. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography. As described below, there is reason to believe that Meek shares these characteristics, that he is engaged in similar activity as these individuals, and that he is engaged in trading and sharing child pornography with individuals sharing these characteristics.

29. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have while viewing children engaged in sexual activity or in sexually suggestive poses, whether in person, in photographs or other visual media, or from literature describing such activity.

30. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or

drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

31. Such individuals may use the internet and cloud storage to allow them to obtain and store the material in relatively secure and anonymous way. However, individuals who have a sexual interest in children or images of children will also often maintain their digital or electronic collections in a safe, secure and private environment on a physical device, such as a computer, flash drive, or phone, as well as in the cloud. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. At times, individuals may leave a bag or case in their vehicle such as a gym or book bag. These items may contain computer storage mediums, a notebook with computer passwords or other related evidence, and paperwork associated with the purchase of a computer device. Thus, I believe there is probable cause to believe that Meek will have child pornography on devices such as computers or hard drives kept within his residence.

32. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis; however, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

33. Such individuals also may correspond with and/or meet others to share

information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

34. Such individuals may prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if a person uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in the person's home.

35. Particularly in light of the fact that Meek has been engaged in child pornography uploading and/or sharing and trading for a period of years, as evidenced by the two 2016 CyberTips and the 2021 Dropbox CyberTip for accounts connected to Meek, the number of child pornography videos (five) that had been stored on Meek's Dropbox account, and the files indicating that Meek was engaged in trading child pornography, based on my training and experience, I believe there is probable cause to believe that Meek will have either other child pornography on his devices, or other evidence of his access, viewing, receipt, and/or distribution on these devices.

F. Surveillance of the SUBJECT PREMISES

36. On or about November 24, 2021, physical surveillance was conducted near the **SUBJECT PREMISES**, and the physical description of the building and apartment door was obtained. Law enforcement also observed Meek's name on the apartment building's directory. As of April 15, 2022, the U.S.P.S. confirmed that mail addressed to Meek was still being delivered to the **SUBJECT PREMISES**.

37. The manager of the apartment building was interviewed, and the manager provided a layout of the apartment. During the course of the interview, law enforcement noted that Meek was listed as an occupant of Apartment [redacted]

SEARCH AND SEIZURE OF COMPUTER SYSTEMS

38. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information of the Target Offenses that might be found on the **SUBJECT PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or on other electronic storage media or digital devices. As used herein, the terms "electronic storage media" and "digital devices" include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of electronic storage media and digital devices or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

39. *Probable Cause.* Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that if electronic storage media or digital

devices are found on the **SUBJECT PREMISES**, there is probable cause to believe that the records and information described in Attachment B will be stored in the electronic storage media and digital devices for at least the following reasons:

a. Based upon my knowledge, training, and experience as well as my discussions with others involved in child pornography investigations, I know that computers and computer technology have revolutionized the way in which child pornography is produced, distributed, received and possessed.

b. Individuals who engage in online criminal activity, including the TARGET OFFENSES, utilize the Internet and computers to allow them to obtain the material in a relatively secure and anonymous way. Individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or flash drive. These collections are often maintained for several years and are kept close by, usually at the collector's residence. Individuals with a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

c. Individuals who engage in the foregoing criminal activity, in the event that they change computers, will often "back up" or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

d. Computer, smart phone, and other digital device files, or remnants of such files, can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to an electronic storage medium can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer or a smart phone, the data contained in the file does not actually disappear; rather, that data remains on the electronic storage medium until it is overwritten by new data.

e. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the electronic storage medium that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from an electronic storage medium depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

f. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic

evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

40. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where,

and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera).

The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to possess, receive, or distribute child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

41. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination*. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it

will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Subject Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro and macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, CDs, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons.

42. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying

storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

43. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

USE OF BIOMETRICS TO UNLOCK DEVICES

44. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint,

thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following.

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on

devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a

short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

45. Based on the above information, I submit there is probable cause for a warrant to

search the **SUBJECT PREMISES** described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

Laura R. Calvillo
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to by telephone
in accordance with Fed. R. Cri. P. 4.1
this 22nd day of April, 2022.

John F. Anderson Digitally signed by John F. Anderson
Date: 2022.04.22 15:16:06 -04'00'

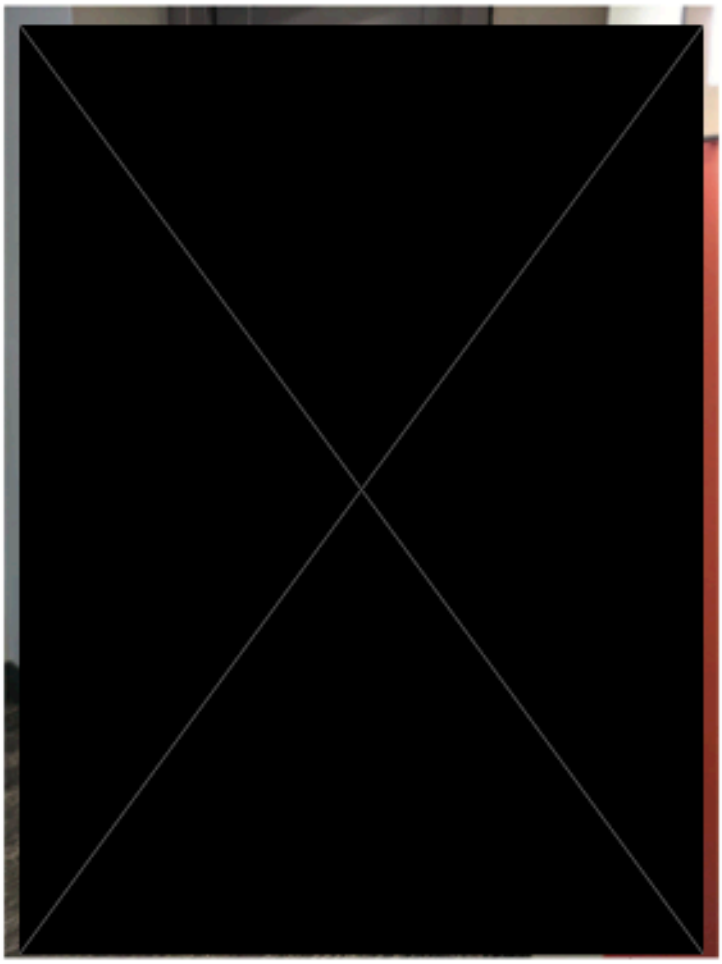
The Honorable John F. Anderson
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

[redacted] (hereinafter, the "SUBJECT PREMISES"), which is an apartment complex [redacted]

Apartment [redacted] which is located on the [redacted] floor of the building is a corner unit and has a dark colored door with a silver door handle and peephole. To the right of the door is a plaque with [redacted] printed on the plaque.



ATTACHMENT B

Items to Be Seized and Searched

1. All records, including those stored digitally, that constitute evidence, instrumentalities, contraband, or fruits of violations of Title 18, U.S. Code, Sections 2252(a)(1) (transportation of child pornography), 2252(a)(2) (receipt and distribution of child pornography), and 2252(a)(4)(B) (possession of child pornography), those violations involving James Meek, including:

a. Records and information relating to images or videos of suspected child pornography;

b. Records and information relating to images or videos of child erotica;

c. Records and information relating to visual depictions of minors engaged in sexually explicit conduct;

d. Records and information relating to communications between Meek and others about child pornography;

e. Records and information relating to the existence of sites on the internet that contain child pornography or that cater to those with an interest in child pornography;

f. Internet usage records, user names, logins, passwords, e-mail addresses, and identities assumed for purposes of communication on the Internet, billing, account, and subscriber records, chat room logs, chat records, membership in online groups, clubs or services, connections to online or remote computer storage, and electronic files;

g. Address books, names, and lists of names and address of individuals who may have been contacted by the computer and internet websites;

h. Records and information relating to membership in online groups, clubs,

or services that provide or make accessible child pornography to members;

i. Records and information relating to any online storage or communication accounts (including, but not limited to, Google accounts, Dropbox accounts, Skype accounts, and Twitter accounts) used to view, access, store, trade, or distribute child pornography;

j. Records and information relating to communications with Internet Protocol addresses [redacted]

k. Records and information relating to the use, control, ownership, or occupancy of the SUBJECT PREMISES and things therein, including, but not limited to, utility and telephone bills, rental purchase or lease agreements, keys, or photographs;

l. All containers in which the items described above may be stored, including, but not limited to briefcases, backpacks, bags, shoe boxes, hampers, laundry baskets, safes, storage containers, storage units, lockers, foot lockers, or tool boxes;

m. Records and information relating to malicious software;

n. Records and information that constitute evidence of the state of mind of James Meek, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and

o. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with James Meek about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.

2. Digital devices used in the commission of, or to facilitate, the above-described offenses, including transporting, distributing, receiving, and possessing child pornography in violation of 18 United States Code Section 2252(a)(1), 2252(a)(2), and 2252(a)(4).

3. For any digital device whose seizure is otherwise authorized by this warrant, and any digital device that is capable of containing and reasonably could contain records or information that is otherwise called for by this warrant (hereinafter, "Device"):

a. evidence of who used, owned, or controlled the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

b. evidence of software, or the lack thereof, that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

d. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

e. evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;

f. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;

g. evidence of the times the Device was used;

h. passwords, encryption keys, and other access devices that may be necessary to access the Device;

i. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device;

j. records of or information about Internet Protocol addresses used by the Device;

k. records of or information about the Device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

l. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "Digital Device," or "Device," encompasses both computers and electronic storage media. The term "computers" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. And, the term "electronic storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM,

floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the Subject Premises described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that an occupant state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel an occupant to state or otherwise provide that information. However, the voluntary disclosure of such information by an occupant is permitted. To avoid confusion on that point, if agents in executing the warrant ask an occupant for the password to any device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

If the government identifies seized materials that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e. communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (*e.g.,* the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team. This investigation is presently covert, and the government believes that the subject of the search is not aware of this warrant.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.